

Every Breath You Take

Deloitte Australia Privacy
Index 2022

MAKING AN
IMPACT THAT
MATTERS

since 1845

Contents

"In this complex environment, it is no longer sustainable to expect individuals to be on constant guard to protect the security and integrity of their personal information. Australia's privacy framework - and organisations entrusted with personal information who operate within in - must protect this data upfront."

Office of the Australian Information Commissioner, Submission on the Privacy Act Review Discussions Paper, December 2021

- ① Foreword
- ② About the report
- ③ Key findings
- ④ Top five takeaways
- ⑤ Privacy Index 2022
- ⑥ Transparency and sharing of information
- ⑦ Online surveillance and location data
- ⑧ Personalised online experiences
- ⑨ Methodology
- ⑩ References
- ⑪ Contacts

1. Foreword

As we begin to emerge from the pandemic, the increased awareness of what data is being shared and with whom has become a global topic. This period of change comes at a time of regulatory reform in Australia. Our world has evolved, our businesses have transformed, and we are embarking on a journey that will outline how our personal information handling practices will change. Over the years, a multitude of jurisdictions have faced regulatory reform within the privacy world. These reforms have led to an adaptation of how both businesses and governments process consumers' data, and an increased awareness amongst consumers about data handling practices.

This year's index is titled "Every Breath You Take", looking at how consumers have gone about transacting over the last two years in a world of increased surveillance (by both government and businesses) arising from the pandemic. Many of us have had to share personal information in exchange for various freedoms and online services driving privacy considerations to the forefront of people's minds. We need to understand what impact this has had on consumer sentiment and expectations on how governments and businesses should interact with them.

One of the key findings from the Index is the emphasis consumers are placing on trust as a foundational element of feeling comfortable with interacting with organisations. This is seen through the following:

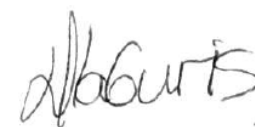
- Consumers voting for choice in data sharing
- Consumers objecting to data being sold
- The rise in the public consciousness of the power of data
- The search for a balance between personalisation and transparency

Across the Australian market, we have seen a rapid increase in the use of tracking and advertising technologies. Organisations are seeking to engage with consumers in a more meaningful way and are often using personalisation techniques to attempt this.

Personalisation is a recurring theme across the Index this year. How many consumers want it versus what they would like in return for the additional information they may share? How will this impact a brand's personalisation journey and what would be considered too far? When does an organisation's actions cross the 'creepy line'?

A key insight of this year's Index is that consumers want personalisation, but they need to be taken on a transparency journey to effectively build trust.

At Deloitte we call this 'Trust First' – an approach to delivering products and services that consider the value of transparency and responsible data handling practices in all interactions with consumers.



Daniella Kafouris

Partner
Deloitte



Kate Monckton

Partner
Deloitte

1

2

3

4

5

6

7

8

9

10

11

2. About the report

Introduction

The amount of information created and copied globally continues to grow and is forecast to increase for many years to come. The COVID-19 pandemic expedited this growth as we moved to learning, working, and entertaining from home. Unfortunately, accompanying this growth has been an increase in associated 'creepy' uses of information. Through the rise of online behavioural monitoring, brands now have access to even more data about their customers. They can act on this information through the personalisation of offers, online experiences and use of advertising tools provided by the likes of big technology corporations and social media.

As a result, in this Index we focus on:

- Transparency and sharing of information by brands compared to consumer expectations.
- Consumer sentiment towards online surveillance and use of location information.
- How consumers value personalised online experiences.

Transparency and sharing of information by brands

One of the key themes in this year's Index is transparency. Consumers can only make decisions about their personal information when they are informed about what it will be used for. We ask consumers about how often they read brand privacy policies or privacy notices and whether the type of information requested leads them to look for greater transparency about how their information will be handled. We also investigate whether consumers are more comfortable sharing their personal information with certain industries and what incentives from brands would encourage them to share their personal information.

We compare this against our brand research, reviewing privacy policies and privacy notices and websites for transparency around the collection and sharing of consumer personal information.

Online surveillance and location information

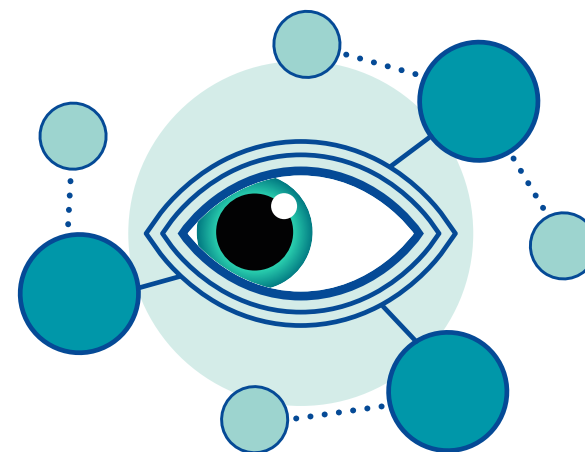
For the purpose of this Index, we define online surveillance as a brand's use of tools to monitor an individual's online behaviour or webpage traffic to gain greater insight into their customers. Online surveillance tools can include location tracking, as well as stitching together an individual's browsing history to generate habit and preference information. In this Index, we ask consumers:

- Whether they think their online behaviour is tracked and what they think a brand may use that information for.
- Whether they think the tracking of online behaviour has changed over time.
- Their behaviours and perceptions around the use of location-based services.

We also analysed the privacy policies, privacy notices and websites of 100 of Australia's leading consumer-facing brands to understand their current online surveillance practices and whether these practices are transparently communicated to consumers.

Personalised online experiences

We set out to determine the perceived privacy value exchange offered to consumers, exchanging control over their personal information for the benefit of personalised online experiences. We ask how happy or unhappy consumers are in seeing advertising and online services tailored to their online behaviour and how much value they place on receiving personalised online experiences. We use that information to define "the Creepy Line", which represents the point at which collection and use of online information becomes creepy to consumers.



1

2

3

4

5

6

7

8

9











10

11

The Index

This year we analysed brands by assessing the transparency around their data sharing and online information collection practices through their websites, privacy policies and annual reports. We reviewed each website and privacy policy against transparency best practices, including simplicity of language, presentation of the Australian Privacy Principle 5 (APP 5) privacy notice and commitment to communicating data uses throughout the customer sign up experience. We reviewed each brand's annual report (where available) to understand the importance placed on using information and innovative technologies, such as the internet of things (IoT) and artificial intelligence (AI), compared to their privacy promises to consumers. From this information we were able to draw interesting comparisons across industry groups between the importance placed on the processing of personal information and upholding consumers' privacy. We combined these findings with selected findings from the consumer survey, as well as sector level breach and complaints data published by the OAIC. The results were scored and aggregated across 10 industry groups enabling us to rank each industry to create the Index.

The ten industry groups include:

-  Education and Employment
-  Energy and Utilities
-  Finance
-  Government
-  Health and Fitness
-  Information Technology
-  Real Estate
-  Retail
-  Telecommunications and Media
-  Travel and Transport

Throughout the report we have used the word “brand” to refer to any organisation that falls under any of the 10 industry types.

Results

We surveyed 1000 Australian consumers over the age of 18 who are demographically representative of the Australian population. All survey responses are confidential and anonymised. The Index and this accompanying report aggregate responses statistically to provide insights into key transparency, data sharing and online surveillance practices across the 10 identified industry groups compared to the expectations of consumers.

Acknowledgements

We would like to acknowledge the following people for their support:

- Dynata, LLC for conducting the consumer survey on behalf of Deloitte.
- The participants of the consumer survey for providing their responses.

1

2

3

4

5

6

7

8

9

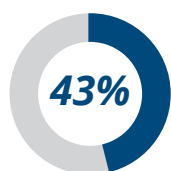
10

11

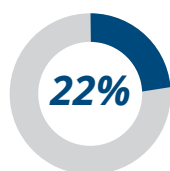
3. Key findings



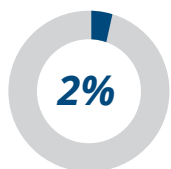
Transparency and Sharing of Information



of consumers indicated that they are happy to share their personal information when they are aware of how their information will be used



of brands have an explanatory privacy webpage on their website where consumers can find out how their information is being used, beyond a brand's privacy policy.



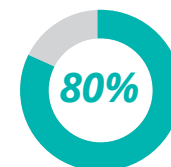
Only 2% of brands use logos, icons or messages that call out data sharing, online tracking, or other specific uses of data during the customer sign-up journey.



Consumers are most comfortable sharing their personal information online with Government agencies and least comfortable sharing with the Real Estate industry.



Personalised online experiences



of consumers saw value in online personalisation

but only



were happy with their current experiences of online personalisation.



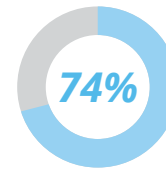
Over 54% of brands offer no tangible incentive to consumers in exchange for creating an account, beyond access to products or services.



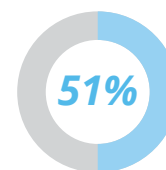
Only consumers aged 18-34 see the value in online personalisation. Consumers aged 35+ see this activity as beyond the Creepy Line.



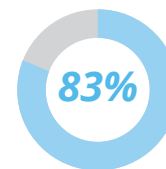
Online Surveillance and Location Information



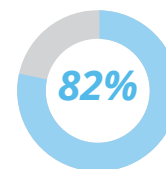
74% of consumers think that brands they interact with online collect browsing information about their online activities.



of consumers are uncomfortable with their activity being subjected to online surveillance.



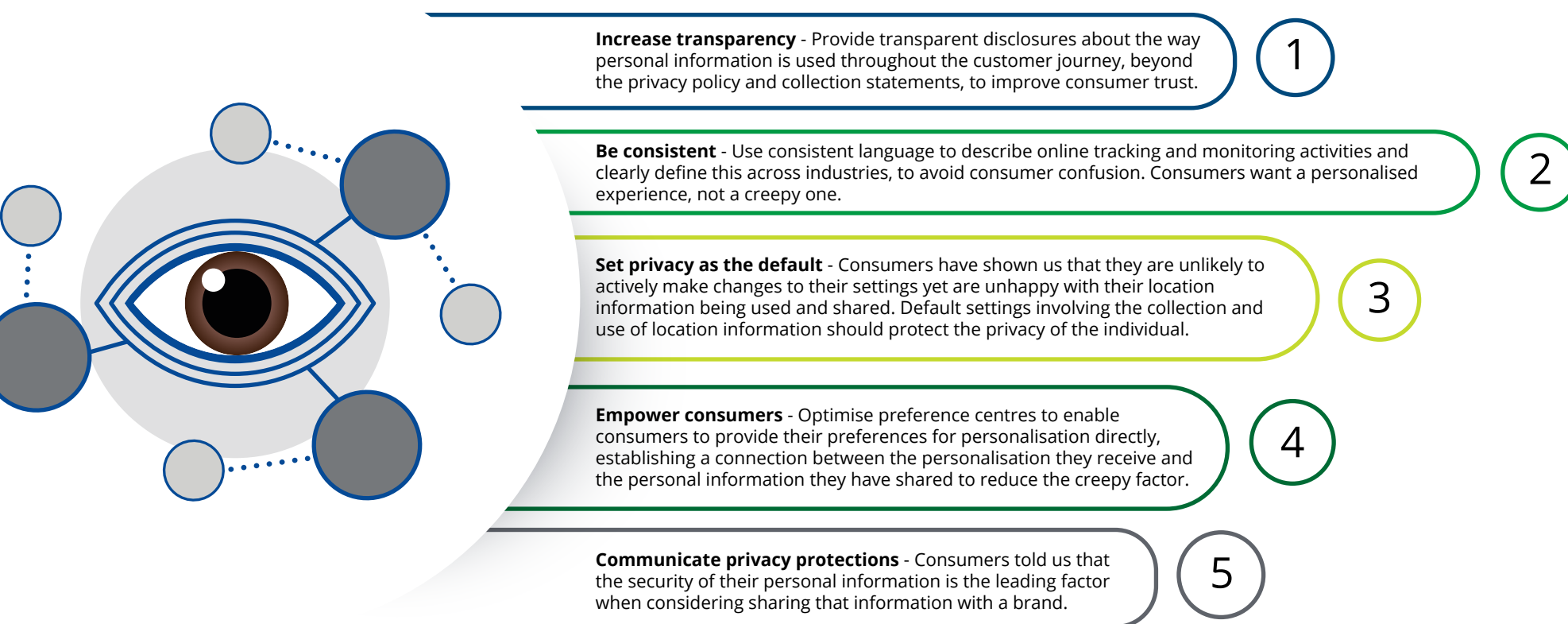
of brands disclose that they conduct online tracking and monitoring activities within their privacy policy.



of consumers are unhappy with their location information being shared with other brands.

4. Top five takeaways

Based on our research, we think brands should do these five things:



1

2

3

4

5

6

7

8

9

10











11

5. Privacy Index 2022

Deloitte Australian Privacy Index 2022 analyses the state of privacy, with a focus on transparency, data sharing and online surveillance practices, of Australia's leading consumer brands across 10 brand sectors. This ranking indicates the overall performance within this privacy element.

5.1 Overall Index

Table 1 The Deloitte Australia Privacy Index 2022

Current Ranking		Previous Ranking		
Index Focus	EVERY BREATH YOU TAKE	Future of Privacy	Consent	Apps
Sector	2022	2021	2020	2019
 Education & Employment	1	4	6	6
 Financial Services	2	8	9	9
 Travel and Transport	3	3	4	3
 Real Estate	4	6	5	2
 Government	5	2	2	8
 Information Technology	6	1	3	1
 Telecommunication & Media	7	10	8	7
 Energy & Utilities	8	9	7	4
 Retail	9	5	1	5
 Health & Fitness	10	7	10	10

Each year the Privacy Index focuses on a different privacy element and, as such, should not be treated as a like for like comparison. The comparison of industries is based on the analysis of how they perform in relation to this year's topic. The rankings provide a holistic view of each industry's privacy posture across each of the focus areas from previous Index editions. For example, the Retail sector had leading consent practices (as of 2020) but performed poorly in surveillance and online personalisation.

By focusing on transparency in online surveillance practices in the 2022 Privacy Index, the sector rankings have shifted. Education and Employment leads the 2022 Privacy Index through a combination of transparency practices that go beyond the Australian Privacy Principle (APP) 5 privacy notice requirements (when compared with other industries) and trust from consumers in those brands protecting their personal information. Financial Services has jumped from 8th to 2nd position demonstrating that, as an industry, they are more transparent about their use of information collected through online surveillance (as of 2022) than they are prepared for the future of privacy (as of 2021).¹ For Government, although the sector scored highly in consumers' trust in the protection of their online information (Figure 1) and transparency about the indirect collection of personal information, the number of privacy complaints to the OAIC about the Australian Government has increased, resulting in a lower ranking.

Trust in protection of online information

This year we asked 1,000 consumers which industry they trust the most and which they trust the least to protect online information collected about them.

These results have been aggregated, returning a net negative or positive trust score for the protection of online information for each industry.

Figure 1 Industries consumers trust most and least for the protection of their online information

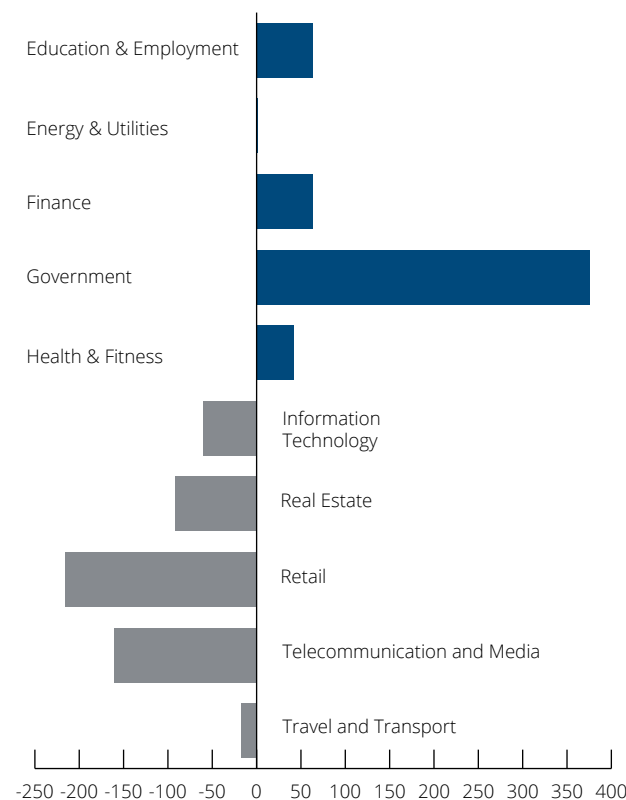


Figure 1 shows that Government is the most trusted industry by consumers for the protection of their online information, with almost 400 more consumers listing Government as their most trusted industry than least trusted. The least trusted industries by consumers for protecting their online information are Retail and Telecommunication and Media. Australian Governments handled various initiatives connected to the Covid-19 pandemic, such as relief or support measures, contact tracing and the provision of Covid-19 vaccinations. While this may not necessarily have caused an increase in trust, generally the Australian population may be comfortable with sharing their personal information to Government agencies. For Retail and Telecommunication and Media, consumers may not trust the rapid transition to online shopping or online consumption of media, as these industries have rushed to establish their online presence in a limited regulatory environment.

¹ Deloitte, 'Deloitte Australia Privacy Index 2021 - Seeing beyond the surface: The future of privacy in Australia', May 2021

6. Transparency and sharing of information

As our lives are becoming increasingly digitised, consumers are more aware of what personal information they share. Our research indicates that consumers want greater transparency about how their personal information is being collected and used by brands.

Transparency as the foundation of trust

More of our day-to-day lives are shifting online with industries digitising their products and services. With this, consumers are becoming more aware about what personal information is being collected and used, which means transparency over information sharing is key to building consumer trust.

As shown in Figure 2, **70%** of consumers surveyed indicate that they sometimes or always read privacy policies before providing their information to a business. This is a **7%** increase since 2019, where **63%** of consumers indicated they read at least part of a privacy policy.²

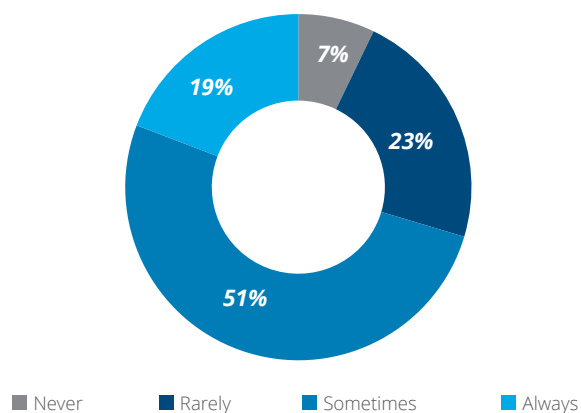


Figure 2 Percentage of consumers reading a privacy policy or collection statement

Additionally, **73%** of consumers indicate that the type of information collected would impact whether they would read the privacy policy or privacy notice. Those consumers state that the types of information most likely to motivate them to read a privacy policy are:

01. Activity/ habit information (for example, online browsing activities, location information)
02. Bank details
03. Government identifiers

This rise in consumer desire to understand data practices should encourage brands to communicate this information through transparent and accessible means. Our analysis shows that **22%** of brands have a privacy centre webpage that uses simple and transparent language, going beyond the privacy policy or privacy notice to make customers aware of how their information is used. The OAIC has recommended the use of standardised icons or lexicon to assist individuals in making informed decisions about their personal information.³ However, our brand analysis found that only **2%** of brands use phrases, logos, and icons during the customer experience sign-up journey to communicate data practices. Brands should consider implementing such measures to help communicate key privacy practices throughout the customer journey in a clear and meaningful way.

At times, brands may collect personal information about an individual from another individual, organisation or source, rather than directly from the individual the information is about. Entities that collect personal information indirectly must take reasonable steps to make the individual aware of APP requirements.⁴ Doing so promotes transparency about information collection and ensures individuals are aware of their rights of access in the collection of their personal information. Our brand analysis results show that **70%** of brands mention indirect collection in their privacy policy or privacy notice. This includes, **32%** that provide a generic statement on indirect collection, such as “there may be circumstances where information may be provided on your behalf, such as from third parties”. This is concerning because these generic statements fail to specify the type of information collected or its intended use, suggesting that brands are indirectly collecting information but are not informing consumers about how and why this information is being collected.

² Deloitte, ‘Deloitte Australia Privacy Index 2021 - Seeing beyond the surface: The future of privacy in Australia’, May 2021

³ OAIC, ‘Submission on the Privacy Act Review Issues Paper’,

⁴ OAIC, Australian Privacy Principles, ‘Notification of the collection of personal information’



Under the Australian Privacy Act, APP 5 requires that an APP entity that collects personal information about an individual, either directly or indirectly, must take reasonable steps in notifying the individual of matters pertaining to their information, or otherwise ensure that the individual is aware of those matters. These matters include, but are not limited to, the fact and circumstances of collection and the purposes of collection.

Our brand analysis suggests that the industry most compliant with the sharing of APP 5 privacy notices detailing the purposes of collecting their personal information prior to sign up was Education and Employment, whilst the least compliant was Energy and Utilities.

Of the brands analysed, only **63%** provide some form of an APP 5 privacy notice for consumers. This breaks down to **49%** that provide consumers with a link to the notice without any additional context about the way the brand collects and handles personal information, **11%** that provide a link with some additional context and only **3%** that display the notice fully on screen. These results are cause for concern as consumers are unlikely to be clearly informed of the reasons behind the collection and use of their personal information.

Collection notification has been identified as a key area for regulatory reform by the Privacy Act Review Discussion Paper published by the Attorney-General's department, which proposed a significant tightening of the situations in which organisations are permitted not to give a privacy notice. "This would require notification at or before the time of collection, or if that is not practicable, as soon as possible after collection, unless:

- the individual has already been made aware of the APP 5 matters; or
- notification would be impossible or would involve disproportionate effort."⁵

This is a risk for brands who do not currently provide a collection notice, as this would be seen as a contravention of APP 5 requirements.

The age of information sharing

The way we work, shop, and socialise has significantly changed over the past decade, with more reliance on our smart devices and the applications within them. As a result, consumers are sharing large amounts of personal information with brands every day. We surveyed consumers to understand the circumstances in which they are willing to share their personal information.

We also researched brands to determine how, if at all, they explain data sharing practices to their customers.

We asked consumers to rank how comfortable they are to share personal information online with the 10 industry types identified (Table 2). Results indicate consumers are most comfortable with sharing personal information with Government agencies, followed closely by those within the Education and Employment industry. Conversely, consumers were least comfortable sharing their personal information with the Retail and Real Estate industry.

Table 2 Industries consumers are most to least comfortable with sharing personal information online

Which industries you are most willing to share your personal information online with:	Comfortableness Score (/10)
 Government	7.4
 Education and employment	6.9
 Energy and utilities	6.6
 Finance	5.9
 Health and fitness	5.2
 Telecommunications and media	5.1
 Travel and transport	5.1
 Information technology	4.2
 Retail	4.2
 Real estate	4.1

⁵ Attorney-General's Department, 'Privacy Act Review Discussion Paper' October 2021. Pg 73



In the survey we conducted, consumers were prompted to share some of the top factors and considerations that impact their decision to share personal information. The top considerations and factors include the security of their personal information, knowledge, and awareness of the brand and their reputation, and the purpose of sharing their personal information.

The practice of data sharing between brands is a point of concern for many consumers, as the personal information they choose to share with one brand may be shared with others, including social media brands for targeted advertising. As shown in Figure 3, **63%** of brands include a generic statement in their privacy policies or privacy notice describing that personal information is shared with third parties. Only **31%** of brands explicitly list the third parties the personal information is shared with by name in the privacy policy or privacy notice.

How are third party disclosures mentioned in your privacy policy?

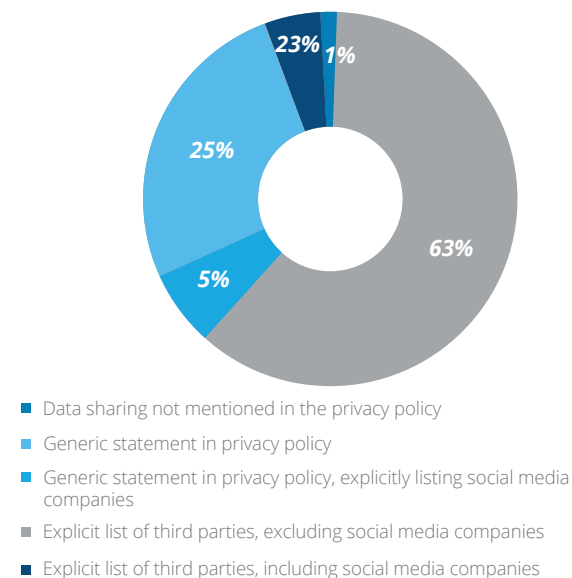


Figure 3 Brands making consumers aware of disclosures with third parties

Interestingly, **43%** of consumers indicate that they are happy to share their personal information when they are aware of how their information will be used, compared to only 21% when they are not made aware of how their information is used. This demonstrates that greater transparency from brands can encourage increased sharing of information from consumers.

Information sharing in the face of Covid-19

We asked consumers to consider how their attitudes towards data sharing had changed since the Covid-19 pandemic, specifically in relation to sharing personal information with brands, Health-care providers and Government agencies. The results indicate that over half of consumer perceptions towards information sharing with brands, Government agencies and Health-care providers remain unchanged, as they maintain they have always been cautious about sharing information. For the remaining consumers who have experienced a change in attitude towards information sharing, we found that they are less willing to share information with brands, but more willing to share this information with Government agencies and Health-care providers (Figure 4).

During the pandemic, consumers were required to share their personal information to protect public health and safety, and thus the sharing of personal information with Government agencies and Health-care providers may have been normalised for this portion of the population. Considering these reduced levels of consumer willingness to share personal information with brands, brands should look to enhance transparency surrounding data usage practices to improve consumer trust.

Are you more willing or less willing to share personal information with the following entities since the start of the pandemic?

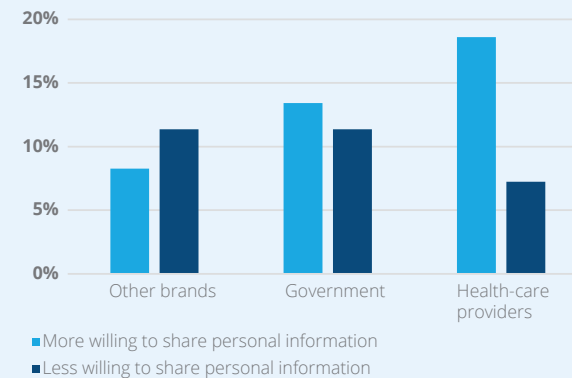


Figure 4 Consumer perspectives on sharing more or less personal information with brands, Government and Health-care providers since the start of the pandemic



1

2

3

4

5

6

7

8

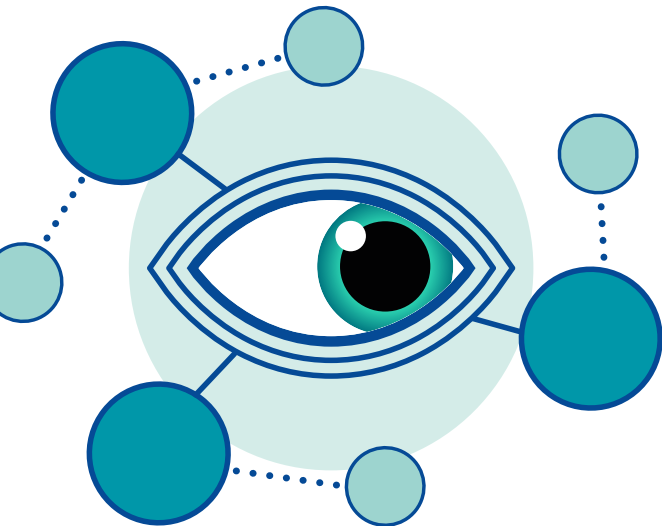
9

10

11

7. Online surveillance and location information

When consumers interact with brands online, their activities, habits and location are often monitored to allow brands to better know their customers. We look to understand how consumers feel about this and what brands can do to build trust with their customers.



Online surveillance

It has become standard practice for brands to use online surveillance technologies to track and monitor consumers' online activities, such as location tracking and browsing activity monitoring. As shown in Figure 5, **74%** of consumers surveyed think that brands they interact with online collect browsing information about their online activities and **20%** are unsure. Of these consumers, **84%** believe that online surveillance has increased over time.

Do you think brands you interact with online collect browsing information about your online activities?

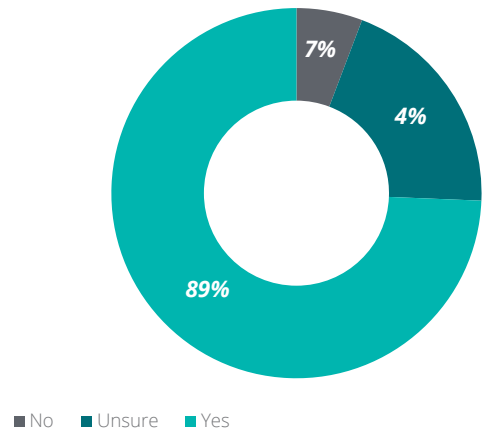









Figure 5 Percentage of consumers who think browsing information is collected online

Consumers were asked to indicate the types of browsing information they think brands collect about them online, and these responses include:

Types of browsing information	Percentage
 Items purchased and purchase history	73%
 Pages visited on their website	71%
 Length of time on the page	58%
 Website that you arrived from	48%
 Website that you went to next	44%
 Social media profile information	36%
 Mouse cursor and location on page and hover time	29%



It is interesting to see that a significant portion of consumers (**from 29% to 73%**) indicate that they suspect brands are collecting browsing information, across all the different types that may be collected. This demonstrates a fairly high perception of awareness of the kinds of information that may be collected, despite our finding that most brands have not included detail about these specific activities (for example, length of time on a webpage or cursor location) in their privacy policies and privacy notices.

As shown in Figure 6, when consumers were asked why they think brands collect this information, **56%** of consumers believe it is for email marketing and to increase sales, **51%** of consumers think it is for analytics and reporting, and interestingly, **51%** of consumers believe their information is being sold to other brands. Regardless of whether brands are engaging in these practices, the general perception held by consumers is that these activities are taking place with or without their knowledge. To alleviate these concerns, brands should explicitly describe in plain language what activities are and are not taking place with regards to the indirect collection of personal information.

In contrast, only **28%** of consumers think their information is collected for the purpose of website personalisation and **32%** believe it is for improving the quality of the brand's offering. This shows consumers are more likely to believe their personal information is collected for the benefit of the brand and are less inclined to think their information is collected to accommodate or benefit the consumer.

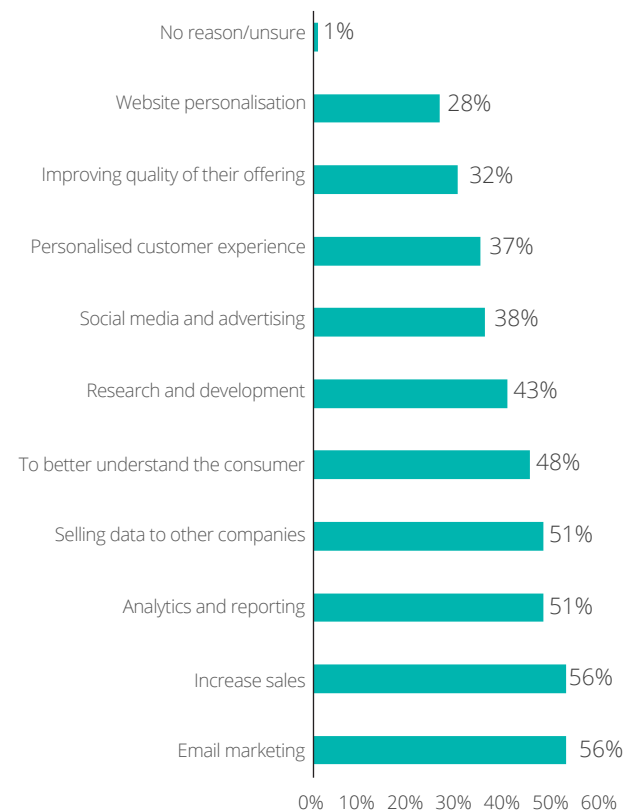


Figure 6 Consumer's perspective on why brands collect information

From reviewing brands' privacy policies and privacy notices, we found that **83%** describe online tracking and monitoring in multiple ways, and the remaining **17%** of brands did not mention if or how they conduct such activities. The brand analysis results show that inconsistent vocabulary was used by brands to communicate online tracking and monitoring activities to consumers, with 12 different terms used. Examples of these include "to deliver targeted advertising based on website visits and page activity" and "help personalise your experience when you visit a website". Brands will often use positive language to frame these activities as being advantageous to consumers, however, this strategy does not appear to be effective in making consumers comfortable with these activities as our research shows **51%** of consumers are still uncomfortable with their activity being subjected to online surveillance.

The lack of consistency in the language used to describe online tracking and monitoring activities may cause confusion amongst consumers. To alleviate the discomfort consumers can have around online tracking and surveillance, brands should be more transparent by plainly describing the online surveillance activities they carry out and offer the opportunity for consumer control, such as managing their preferences around online data collection and targeted advertising, without the consumers' online experience being hindered.

Concerns around location-based services

In 2020, nearly half of Australians considered location information to be one of the biggest privacy risks today and two-thirds of Australians were of the view that most brands target ads based on location information⁶.

As shown in Figure 7, **38%** of consumers are unlikely to share their location with an online service, compared with **28%** of consumers that are likely to share this information when asked. Concerningly, over **60%** of brands do not mention data deletion and account closure within their privacy policy, privacy notice and terms and conditions, and **39%** neglect to include information about their data retention policies. This indicates that once a consumer shares their personal information with these brands, they have little control over the information and that the information may be retained indefinitely. Brand analysis results show that the Health and Fitness industry ranked highest for notifying consumers of data deletion and retention processes in the privacy policy or privacy notice.

How likely or unlikely are you to allow your location to be shared with an online service when asked?

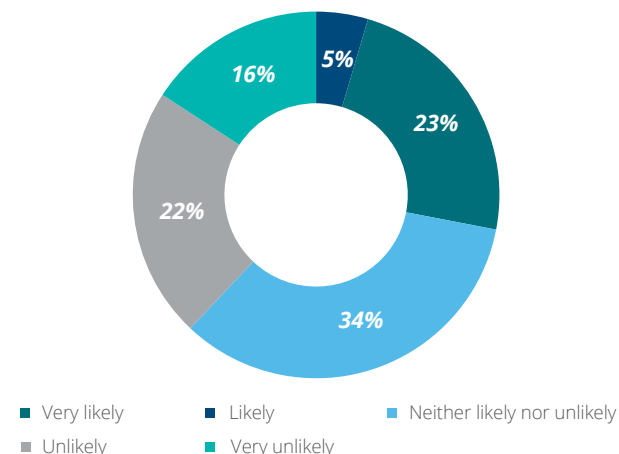


Figure 7 How likely or unlikely consumers are to share location information

⁶ OAIC Australian Community Attitudes to Privacy Survey. September 2020, Pg 78

We asked consumers whether they change their location settings on an app or website after signing up, **25%** indicate they are unlikely to change these settings and **43%** indicate they are neither likely nor unlikely to change them. This suggests that these consumers are not taking action to change their location information sharing preferences. If brands want to improve their location data practices, and they do not require location information switched on for regular business functions, they should consider setting up privacy positive defaults for the sharing of location information in line with the privacy by design principle of setting privacy defaults.

Figure 8 demonstrates that consumers are more unhappy than happy for eight of the ten uses of location information presented to them. This indicates that, overall, consumers show hesitancy and unhappiness towards companies using their location information. Consumers are most unhappy with their location information being shared with other brands (**82%**). The only two uses of location data sharing that are valued by consumers are when done to present them with similar services nearby (**56%**) and the distance to nearby services (**58%**).

How happy or unhappy would you be with a company using your location data for each of the following?

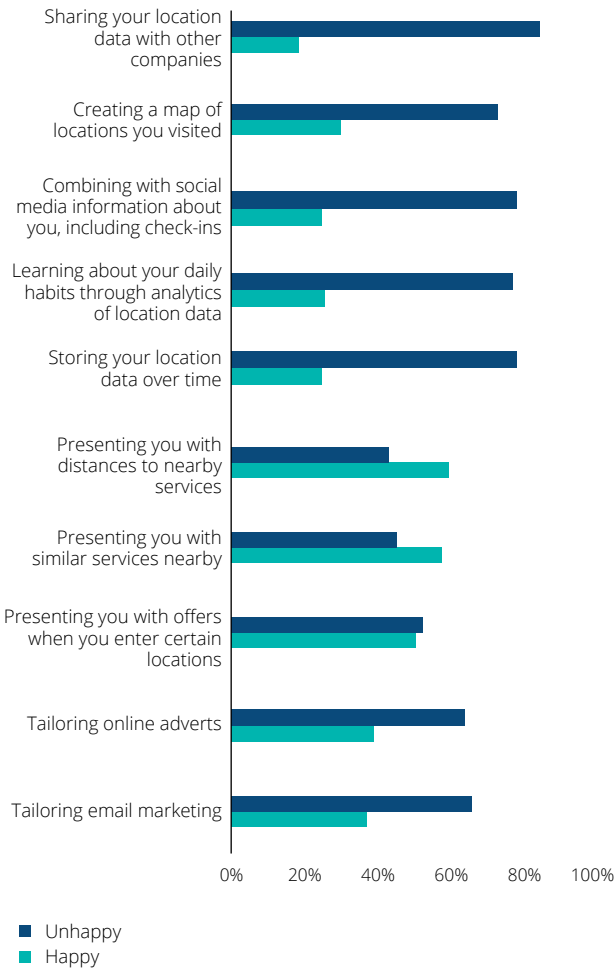
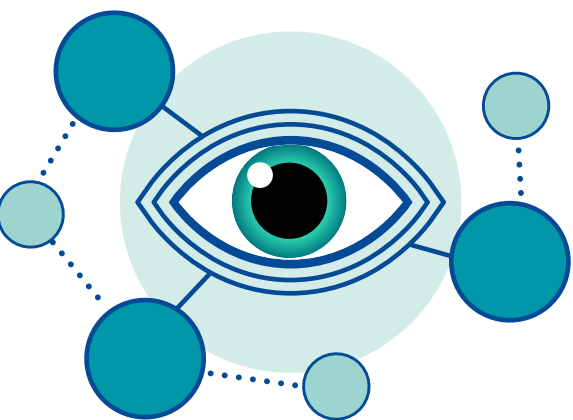


Figure 8 Consumer's level of satisfaction on brands using location information



8. Personalised online experiences

Brands can use browsing information to tailor advertisements and recommend products or services, specific to consumer tastes and preferences, but at what cost to privacy? We ask consumers how they value personalisation and look to define the “creepy line”.



Personalisation

The use of personalisation to improve customer experience is fast growing. Forbes states that “personalisation is fast becoming the cornerstone of best-in-class customer care. Delivering a satisfying brand experience isn't just about knowing which channels and platforms your customers prefer, but also understanding — and even anticipating — their needs in order to provide relevant content.”⁷

Figure 9 shows that **81%** of consumers place some value on online services personalising their experiences to their tastes and preferences.

Do you place value on online services personalising your experience to your tastes and preferences?

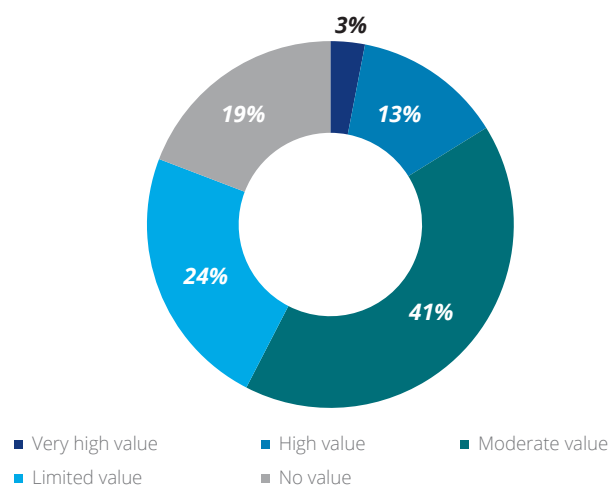


Figure 9 Consumer's perception of value provided by personalised online services

After establishing whether consumers find online personalisation valuable, consumers were asked how they feel about their personalised online experiences, such as streaming services suggesting a watch-list or brands recommending products, compared with personalised online advertising. Interestingly, **30%** of consumers were happy with their personalised online experiences yet only **20%** were happy with receiving personalised online advertising. When compared with the **81%** of consumers that place some value in personalisation, this indicates that brands are not currently delivering personalisation, either through experiences or advertising, in a way that meets consumer expectations.

Brands could improve their personalisation by collecting the information needed to drive this activity directly from the consumers, providing them with a choice of what information is to be used. This can be operationalised using preference centres. Of the brands analysed, **57%** have preference centres available that allow consumers to change the level of marketing they receive, with the Finance sector ranking 1st for having preference centres available and Energy and Utilities, and Real Estate scoring a tied 8th place being less likely to offer this feature. With increased choice and control, more consumers could be happier with the personalised online experiences and advertising they receive.

⁷ Forbes, 'Achieving Personalization Through Data And Analytics', December 2019

Consumer sentiments of personalisation



Figure 10 Comparing how consumers feel about personalised online experiences against personalised online advertising

Personalised online experiences can allow for brands to deliver customer-centric services and create positive experiences for the consumer. However, brands need to consider the balance of providing personalised service and tailored adverts with offering control to consumers in order to create a positive experience for both consumers and brands alike.

Privacy value exchange

In 2019 it was found that “almost 90 per cent of Australian consumers are estimated to be part of a customer loyalty scheme, with the average Australian holding four to six loyalty cards”.⁸

The consumer sentiment survey aimed to understand what factors may incentivise individuals to share personal information more freely and how brands value privacy within their businesses. We asked consumers what outcomes would incentivise them to share personal information and found that a guarantee of secure storage of their information was the leading incentive when considering sharing their personal information, followed closely by a monetary payment in exchange for the information. The fact that security was ranked above tangible benefits shows the importance consumers place on the security of their personal information. The results also show that consumers may be seeking a benefit before sharing their personal information by signing up to an account, and in some circumstances, may expect both security and a tangible benefit.

Most incentivising to least incentivising factors for consumers to share their personal information

01. Guarantee of secure (information) storage
02. (Monetary) Payment
03. Personal health benefit
04. Access to better quality services/products
05. Discount on a service/ product
06. Access to a service/ product
07. Public health benefit
08. Voucher

Results obtained from the brand analysis (Figure 13) show that over **54%** of brands are offering no tangible incentive to consumers in exchange for creating an account, beyond access to services. Only **8%** offer vouchers of some description and **5%** provide direct monetary value for the consumer. It is evident that consumers are seeing the value brands can get from use of their information and want to receive a fair value exchange sharing their personal information. In December 2019, the Australian Competition and Consumer Commission (ACCC) released their findings in relation to customer loyalty schemes. The ACCC recommended reforms to privacy and consumer law around loyalty schemes and the key takeaway from this report are that brands need to ensure that consumers are well informed and receive benefits advertised in the exchange.⁹ Brands should consider whether their current offerings to consumers adequately represent the value of the information they are requesting and ensure they provide proper transparency to consumers before sign-up on the use of their information.

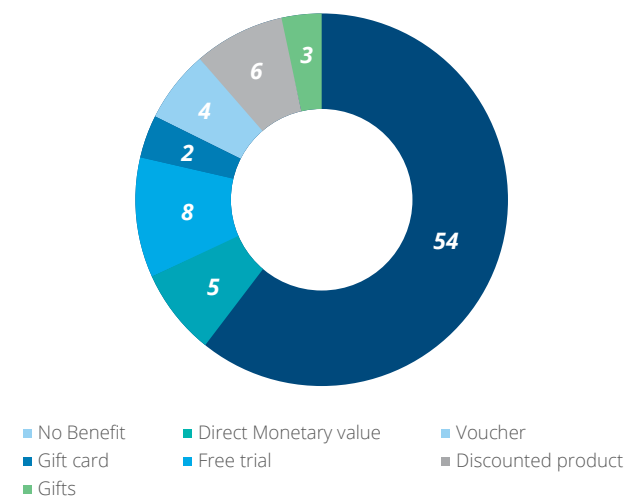


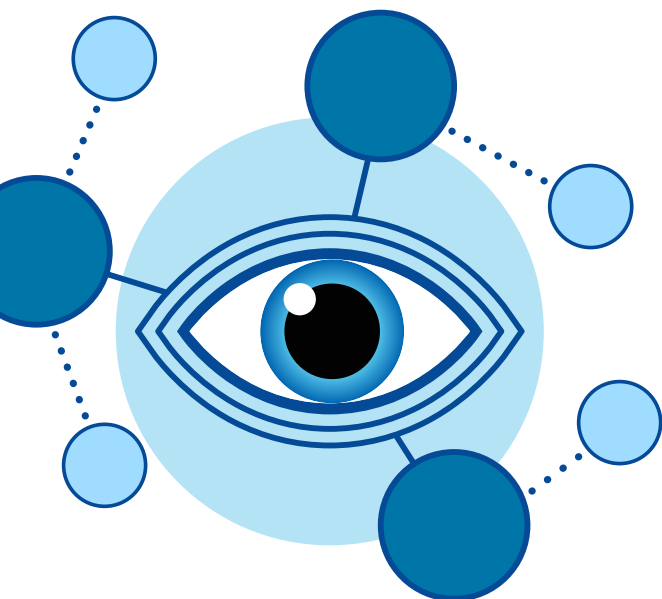
Figure 13 Brand incentives for consumers to create an account

⁸ <https://www.minterellison.com/articles/accc-consumer-protection-customer-loyalty-schemes>

⁹ <https://www.accc.gov.au/publications/customer-loyalty-schemes-final-report>

The Creepy Line

We sought to understand the balance between consumers finding personalisation helpful and what could be considered “creepy”, hindering the customer experience and a brands ability to build trust with consumers. To establish the Creepy Line, we asked consumers to indicate their happiness and/or comfort level with seven common data sharing situations.



The Creepy Line

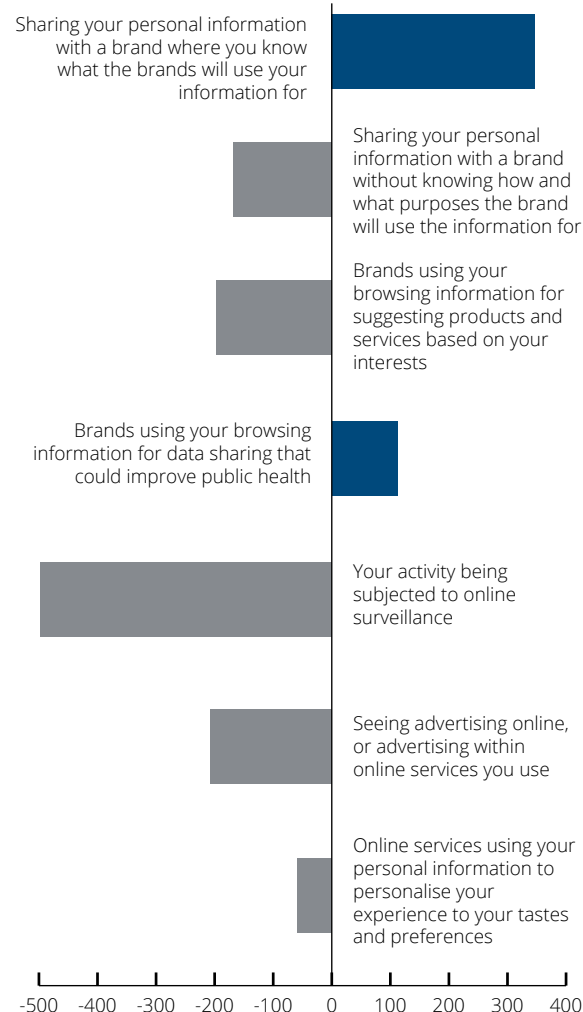


Figure 14 Establishing the Creepy Line. At what point is personalisation helpful or valuable, and when is it considered creepy?

Figure 14 shows consumers believe that sharing their information with a brand where they know what the brand will use their information for and brands using their browsing information for data sharing which could improve public health, are features consumers consider to be helpful or valuable. Conversely, our research shows that consumers find their online activity being subjected to online surveillance most creepy.

Interestingly, online services using personal information to personalise experiences to consumer tastes and preferences was placed below the Creepy Line. When we reviewed the demographic breakdown, we saw that consumers aged 35+ found this creepy whereas consumers aged between 18-34 found this helpful. This indicates that brands should consider using the personalisation of online experiences as a benefit to consumers if their target age demographic is 18-34 but should not promote this feature to target age demographics aged 35+ as it is not perceived as a benefit.

9. Methodology



Findings

The Deloitte Australian Privacy Index 2022 analyses the state of privacy, with a focus on transparency, data sharing and online surveillance practices, of Australia's leading consumer brands across 10 brand sectors. The overall ranking of the Index was developed from:

- Analysis of privacy policies and privacy notices of 100 leading consumer brands active in the Australian market.
- Survey responses from more than 1,000 Australian consumers.
- The OAIC Notifiable Breach Scheme Reports (January – December 2021).
- OAIC Annual Report 2021
- Consumer survey results

An external organisation, Dynata LLP, was engaged to survey more than 1,000 Australian consumers, that are demographically representative of the Australian Population, to share their opinions on data sharing and gain insight into their perceptions of online surveillance practices by various brands. The focus was on how consumers feel about sharing of their personal information for a variety of purposes to define “the Creepy Line”.

Brand analysis

We analysed the websites, privacy policies and annual reports (where available) from the top 100 consumer-facing brands in Australia according to a question set developed out of transparency best practices and trends in use of technology to support advertising and personalisation. The brands chosen this year were required to be domiciled in Australia in order to give a more accurate reflection of the maturity of the Australian market, with less influence from the regulations of other jurisdictions. Our views on brands activities have been formulated from the information they disclose in their privacy policies, privacy notices, websites and annual reports.

1

2

3

4

5

6

7

8

9

10

11

10. References

National

- ACCC, 'Customer Loyalty Schemes Review Final Report', December 2019
- Deloitte, 'Deloitte Australia Privacy Index 2019 - Trust: is there an app for that', May 2019
- Deloitte, 'Deloitte Australia Privacy Index 2021 - Seeing beyond the surface: The future of privacy in Australia', May 2021
- Forbes, 'Achieving Personalization Through Data And Analytics', December 2019
- Minter Ellison, 'ACCC recommends protections for consumers using customer loyalty schemes', (<https://www.minterellison.com/articles/accc-consumer-protection-customer-loyalty-schemes>)
- OAIC, Australian Privacy Principles, 'Notification of the collection of personal information', <https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-5-app-5-notification-of-the-collection-of-personal-information>
- OAIC, 'Australian Community Attitudes to Privacy Survey', September 2020
- OAIC, 'Notifiable Data Breaches Report: January-June 2021', August 2021
- OAIC, 'Notifiable Data Breaches Report: July-December 2021', February 2022
- OAIC, 'Submission on the Privacy Act Review Discussions Paper', December 2021
- OAIC, 'Submission on the Privacy Act Review Issues Paper', December 2020'
- Privacy Act 1988 (Cth)

International

- General Data Protection Regulation 2016/679 (EU)
- Regulatory Guidelines and Reports
- EU ePrivacy Directive

Top 100 consumer brands

Sources considered in developing the top 100 Australian consumer brands for analysis:

- Deloitte, 'Deloitte Australia Privacy Index 2021 - Seeing beyond the surface: The future of privacy in Australia', May 2021
- Brand Finance - Top 100 most valuable Australian brands (https://brandirectorypublic.s3.eu-west-2.amazonaws.com/reports_free/brand-finance-australia-100-2022-preview.pdf)
- AFR and IBISWORLD - top 500 private Australian companies, ranked by company revenue (<https://www.ibisworld.com/blog/top-500-companies-2021/61/1133/>)



1

2

3

4

5

6

7

8

9

10

11

11. Contacts

National Partners



Daniella Kafouris

Partner | Risk Advisory | Melbourne
dakafouris@deloitte.com.au



Kate Monckton

Partner | Risk Advisory | Sydney
kmonckton@deloitte.com.au



Judith Donovan

Partner | Risk Advisory | Brisbane
JDonovan@deloitte.com.au



Tom Rayner

Partner | Risk Advisory | Perth
trayner@deloitte.com.au



David Hobbis

Partner | Risk Advisory | Adelaide
dhobbis@deloitte.com.au



Elizabeth Lovett

Partner | Risk Advisory | Hobart
ellovett@deloitte.com.au



Rachelle Koster

Partner | Risk Advisory | Canberra
rkoster@deloitte.com.au



Ian Blatchford

Partner | Risk Advisory | National
iblatford@deloitte.com.au

About the team

The Privacy experts in our Cyber Security Practice who developed the Deloitte Australian Privacy Index 2022 included: Celia Cavanagh, Project Manager; Graham Chikaka, Project Delivery Lead; Imogen Smith-Waters, Project Co-ordinator; Samantha Barr, Project Co-ordinator; Teagan McKenna, Project Writer; Samantha Santa-Isabel, Project Writer; Marie Liskaser, Project Writer.

1

2

3

4

5

6

7

8

9

10

11



This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms or their related entities (collectively, the “Deloitte organisation”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities. DTTL (also referred to as “Deloitte Global”) and each of its member firms and their affiliated entities are legally separate and independent entities. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our network of member firms in more than 150 countries and territories serves four out of five Fortune Global 500® companies. Learn how Deloitte’s approximately 286,000 people make an impact that matters at www.deloitte.com.

Deloitte Asia Pacific

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities provide services in Australia, Brunei Darussalam, Cambodia, East Timor, Federated States of Micronesia, Guam, Indonesia, Japan, Laos, Malaysia, Mongolia, Myanmar, New Zealand, Palau, Papua New Guinea, Singapore, Thailand, The Marshall Islands, The Northern Mariana Islands, The People's Republic of China (incl. Hong Kong SAR and Macau SAR), The Philippines and Vietnam, in each of which operations are conducted by separate and independent legal entities.

Deloitte Australia

In Australia, the Deloitte Network member is the Australian partnership of Deloitte Touche Tohmatsu. As one of Australia's leading professional services firms, Deloitte Touche Tohmatsu and its affiliates provide audit, tax, consulting, and financial advisory services through approximately 8000 people across the country. Focused on the creation of value and growth, and known as an employer of choice for innovative human resources programs, we are dedicated to helping our clients and our people excel. For more information, please visit our web site at <https://www2.deloitte.com/au/en.html>.

Liability limited by a scheme approved under Professional Standards Legislation.
Member of Deloitte Asia Pacific Limited and the Deloitte Network.